AFRL-RI-RS-TR-2013-143

MAKING COMPUTING ON ENCRYPTED DATA SECURE AND PRACTICAL

UNIVERSITY OF CALIFORNIA, IRVINE

JUNE 2013

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2013-143 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /

CARL R. THOMAS
Work Unit Manager

/ S /

MARK H. LINDERMAN
Technical Advisor, Computing & Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
JUNE 2013	FINAL TECHNICAL REPORT	SEP 2011 – JAN 2013

4. TITLE AND SUBTITLE

Making Computing on Encrypted Data Secure and Practical

5a. CONTRACT NUMBER
FA8750-11-1-0248

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62303E

6. AUTHOR(S)

Alice Silverberg

5d. PROJECT NUMBER
PROC

5e. TASK NUMBER
ED

5f. WORK UNIT NUMBER
UC

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of California, Irvine
5171 California Avenue, Suite 150
Irvine, CA 92697

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/RITA
525 Brooks Road
Rome NY 13441-4505

Defense Advanced Research Projects Agency
3701 N. Fairfax Dr.
Arlington, VA 22203-1714

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2013-143

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The project discovers and develops new mathematical foundations for computation on encrypted data, and develops the mathematical underpinnings of fully and somewhat homomorphic encryption, in order to improve the security and efficiency of fully homomorphic encryption schemes.

15. SUBJECT TERMS
Fully Homomorphic Encryption, Somewhat Homomorphic Encryption, Computation on Encrypted Data

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**CARL R. THOMAS**
U	U	U	UU	32	19b. TELEPONE NUMBER (*Include area code*) **N/A**

TABLE OF CONTENTS

Section **Page**

ACKNOWLEDGMENTS

The results in this report are joint work with Hendrik Lenstra. In addition, useful comments were given by Zvika Brakerski, Craig Gentry, Lily Khadjavi, Chris Peikert, and Nigel Smart.

1. Summary

In order to make computing on encrypted data be both practical to use and secure from attack, it is necessary to discover, develop, and understand the mathematics on which it is based. Discovering and developing the mathematical foundations of fully homomorphic and somewhat homomorphic encryption schemes allows computing on encrypted data to be performed with confidence, knowing that its cryptographic security is based on sound mathematical foundations.

Hendrik Lenstra and Alice Silverberg discovered and developed some of the mathematical foundations of some homomorphic encryption schemes, and propose a variant that has some advantages over earlier systems in terms of efficiency. In this variant, the secret key of the encryption scheme is a lattice basis that is nearly orthogonal with respect to a certain measure. This makes decryption very efficient. The cryptographic security of the scheme comes from ensuring sufficient entropy when choosing the basis.

A primary method of attack on homomorphic encryption schemes consists of lattice algorithms performed on ideal lattices. The work performed here uses lattices that have some symmetry. Recommendations are that the mathematical foundations of lattices with symmetry be discovered and developed, in order to help quantify the security of homomorphic encryption schemes.

This material is based on research sponsored by DARPA under agreement number FA8750-11-1-0248. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

2. Introduction

Fully Homomorphic Encryption (FHE) has been referred to as a "holy grail" of cryptography. Craig Gentry's recent solution to the problem, while not efficient enough to be practical, was considered to be a major breakthrough. Since then, much progress has been made in the direction of finding efficient Fully Homomorphic Encryption schemes.

In encryption schemes, Bob encrypts a plaintext message to obtain a ciphertext. Alice decrypts the ciphertext to recover the plaintext. In Fully Homomorphic Encryption, parties that do not know the plaintext data can perform computations on it by performing computations on the corresponding ciphertexts.

A major application of FHE is to cloud computing. Alice can store her data in "the cloud", e.g., on remote servers that she accesses via the Internet. The cloud has more storage capabilities and computing power than does Alice, so when Alice needs computations to be done on her data, she would like those computations to be done by the cloud. However, Alice does not trust the cloud. Her data might be sensitive (for example, Alice might be a hospital and the data might be patients' medical records), and Alice would like the cloud to know as little as possible about her data, and about the results of the computations. So Alice sends encrypted data to the cloud, which can perform arithmetic operations on it without learning anything about the original raw data, by performing operations on the encrypted data.

Fully Homomorphic Encryption can be used to query a search engine, without revealing what is being searched for (here, the search engine is doing the computations on encryptions of information that it doesn't know).

More precisely, FHE has the following property. Say that ciphertexts c_i decrypt to plaintexts m_i, i.e., $\text{Decrypt}(c_i) = m_i$, where the m_i's and c_i's are elements of some ring (with two operations, addition and multiplication). In FHE one has

$$\text{Decrypt}(c_1 + c_2) = m_1 + m_2, \qquad \text{Decrypt}(c_1 \cdot c_2) = m_1 \cdot m_2.$$

In other words, decryption is doubly homomorphic, i.e., homomorphic with respect to the two operations addition and multiplication.

Being fully homomorphic means that whenever f is a function composed of (finitely many) additions and multiplications in the ring, then

$$\text{Decrypt}(f(c_1, \ldots, c_t)) = f(m_1, \ldots, m_t).$$

If the cloud (or an adversary) can efficiently compute $f(c_1, \ldots, c_t)$ from ciphertexts $c_1, \ldots, c_t$, without learning any information about the corresponding plaintexts m_1, $\ldots, m_t$, then the system is efficient and secure.

Another requirement for FHE is that the ciphertext sizes remain bounded, independent of the function f; this is known as the "compact ciphertexts" requirement.

Fully Homomorphic Encryption schemes can be either public key (where the encryptor knows the decryptor's public key but not her private key) or symmetric key

(where the encryptor and decryptor share a key that is used for both encryption and decryption).

H. W. Lenstra and A. Silverberg propose a variant of some somewhat homomorphic encryption schemes that were proposed earlier by others. In this variant, the secret key is a lattice basis that is nearly orthogonal with respect to Gauss's general measure. This makes decryption very efficient. Cryptographic security comes from ensuring sufficient entropy when choosing the basis.

To fix ideas, we use the somewhat homomorphic encryption schemes of Smart-Vercauteren and Gentry-Halevi as our jumping off point. However, the ideas proposed here, and the discussion concerning their security and efficiency, should be useful in studying or implementing other cryptographic schemes.

Decryption in lattice-based encryption schemes relies on the secret lattice basis being better (i.e., more orthogonal) than a basis obtained via the Lenstra-Lenstra-Lovász (LLL) lattice basis reduction algorithm. The lattice bases proposed here are sufficiently orthogonal to give encryption schemes that are more efficient than with previously proposed bases, while maintaining cryptographic security.

In Section 3 we give the necessary background. The results and discussion are in Section 4, and constitute work performed jointly by Hendrik Lenstra and Alice Silverberg. Section 4.1 includes results and discussion concerning decryption. In Section 4.2 we discuss the security of a variant that has been proposed by Vercauteren and Gentry. In Section 4.3 we give some relevant algebraic number theory results, and give a natural inner product with respect to which the bases we construct will be nearly orthogonal. In Section 4.4 we present a first step in the direction of producing suitable nearly orthogonal bases, and in Section 4.5 we discuss the security of associated encryption schemes. In Section 4.6 we give the full variant proposed by Lenstra and Silverberg. In Section 4.7 we give results that justify why decryption works. A discussion of the cryptographic security is in Section 4.8.

The results are joint work with Hendrik Lenstra. Thanks go to Zvika Brakerski, Craig Gentry, Lily Khadjavi, Hendrik Lenstra, Chris Peikert, and Nigel Smart for helpful discussions and comments.

3. Methods, Assumptions, and Procedures

In this section we give the assumptions and background. In Section 3.1 we give some of the terminology, history, and other background. In Section 3.2 we recall a simple illustrative example. In Section 3.3 we recall an encryption scheme for which we will obtain some results in Section 4.

As usual, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ denote the integers, rational numbers, real numbers, and complex numbers, respectively, and $\mathbf{F}_q$ denotes the finite field with q elements.

3.1. **Some history and background.**

3.1.1. *Early history.* In 1978, shortly after the invention of the RSA Cryptosystem, Rivest, Adleman, and Dertouzos [35] came up with the idea of fully homomorphic encryption, which they called "privacy homomorphisms". Their paper states, "although there are some truly inherent limitations on what can be accomplished, we shall see that it appears likely that there exist encryption functions which permit encrypted data to be operated on without preliminary decryption of the operands, for many sets of interesting operations. These special encryption functions we call 'privacy homomorphisms'; they form an interesting subset of arbitrary encryption schemes". Despite the optimism of Rivest, Adleman, and Dertouzos, fully homomorphic encryption remained out of reach for many years.

A number of cryptosystems are homomorphic with respect to one operation. For example, RSA and ElGamal encryption are homomorphic with respect to multiplication.

We recall that in (basic) RSA, Alice's public key is (N, e) and private key is d, where N is a product of two large primes and where $de \equiv 1 \bmod \varphi(N)$. If $m \in \mathbf{Z}/N\mathbf{Z}$ is the plaintext, then the ciphertext is $c = m^e \bmod N$. To decrypt, Alice computes $c^d \bmod N = m$. If Bob encrypts messages m_1 and m_2 using Alice's public key (N, e), then the product of the resulting ciphertexts is the ciphertext of the product of the plaintexts m_1 and m_2, i.e., $(m_1^e \bmod N)(m_2^e \bmod N) = (m_1 m_2)^e \bmod N$. Thus, $\text{Decrypt}(c_1 \cdot c_2) = \text{Decrypt}(c_1) \cdot \text{Decrypt}(c_2)$, where $c_i = m_i^e \bmod N$ is the ciphertext corresponding to the plaintext m_i.

For ElGamal, suppose the private key is $x \in \{1, \ldots, n-1\}$ and the public key is $h = g^x \in G$, where G is a cyclic group of order n generated by g. If $m_1, m_2 \in G$ are plaintext messages, then the corresponding ciphertexts are of the form $c_i = (a_i, b_i) = (g^{r_i}, m_i h^{r_i}) \in G \times G$ for $i = 1$ and 2, where the r_i are chosen by the encryptor(s) at random in $\{1, \ldots, n-1\}$. Then

$$\begin{aligned}\text{Decrypt}(c_1 \cdot c_2) = \text{Decrypt}(a_1 a_2, b_1 b_2) &= ((a_1 a_2)^x)^{-1} b_1 b_2 \\ &= (a_1^x)^{-1} b_1 \cdot (a_2^x)^{-1} b_2 = \text{Decrypt}(c_1) \cdot \text{Decrypt}(c_2).\end{aligned}$$

There have been other encryption schemes with homomorphic properties. For example, the Goldwasser-Micali cryptosystem [21] and its generalization the Paillier cryptosystem [31] are homomorphic with respect to addition of plaintexts in the sense

that

$$\text{Decrypt}(c_1 \cdot c_2) = m_1 + m_2,$$

but are not homomorphic with respect to multiplication of plaintexts.

In [1], Boneh, Goh, and Nissim gave a partially homomorphic encryption scheme that can do one multiplication and any number of additions.

3.1.2. *Gentry's FHE scheme and beyond.* Craig Gentry solved the problem of how to do Fully Homomorphic Encryption in his Stanford PhD thesis [12, 13, 14]. For the first time, there was now a scheme that could (inefficiently) do an arbitrary number of additions and multiplications.

Gentry's solution used ideal lattices, i.e., ideals in algebraic number fields. Given that one requires a homomorphic property with respect to two operations, it is natural that rings come into play. In [12] and [13], the rings Gentry used were of the form

$$R = \mathbf{Z}[x]/\langle x^N + 1\rangle \quad \text{and} \quad R_d = (\mathbf{Z}/d\mathbf{Z})[x]/\langle x^N + 1\rangle$$

where $N = 2^n$ (see Section 3.3 below). It was later realized that one can use the rings $\mathbf{Z}$ and $\mathbf{Z}/d\mathbf{Z}$ to construct schemes parallel to those that use the rings R and R_d (see Section 3.2 below).

There have been a number of improvements, implementations, and new schemes. See for example [36, 11, 15, 37, 16, 25, 17, 6, 5, 9, 28, 4, 18, 19, 10, 3]. The NTRU encryption scheme [23], which was developed in the late 1990's, turned out to be "somewhat homomorphic", and has been turned into an FHE scheme [29].

3.1.3. *Security.* The primary known attacks on FHE schemes are variants of the LLL lattice basis reduction algorithm [27]. The security of almost all currently known schemes is based on the presumed difficulty of some lattice problem, such as finding an approximately shortest (non-zero) vector in a high dimensional lattice.

A number of FHE schemes use ideal lattices rather than arbitrary lattices. These are very special lattices, and it might turn out to be the case that lattice attacks are easier for ideal lattices than for generic lattices. This is an open question. At the moment, special attacks that work better for ideal lattices than for general lattices are not yet known.

3.1.4. *Somewhat Homomorphic Encryption (SHE).* Somewhat Homomorphic Encryption (SHE) schemes are encryption schemes that have some homomorphic properties but are not fully homomorphic. With Somewhat Homomorphic Encryption one can generally do a limited number of additions and multiplications, but each time one does an operation, it contributes "noise" to the ciphertext (see Section 3.2 for an example). Eventually the noise is so great that it is not possible to decrypt. Also, in SHE schemes the ciphertexts could get larger (message expansion), i.e., the compact ciphertexts requirement might be violated. In Gentry's initial work he started with an SHE scheme and then "bootstrapped" it to obtain an FHE scheme.

3.1.5. *Bootstrapping.* Gentry's original FHE papers and thesis introduced the idea of bootstrapping. One "bootstraps" to go from a (bootstrapable) somewhat homomorphic encryption scheme to a fully homomorphic encryption scheme.

To make an SHE scheme fully homomorphic, one can include as part of the public key an encryption of the private key. When a ciphertext gets too large or too noisy, the encryptor can then use the somewhat homomorphic encryption scheme to evaluate the decryption function applied to the ciphertext, using the encrypted private key. This re-encryption process produces a new encryption of the original plaintext, that is more compact and less noisy. For this to work, it is necessary for the somewhat homomorphic scheme to be "circular secure" (i.e., it must be able to securely encrypt its own private key) and capable of (homomorphically) evaluating the function $f =$ Decrypt and "a little more". Here, we view the argument of the Decrypt function as being the secret key, rather than the ciphertext, and we view the ciphertext as fixed.

Gentry also uses what he calls "squashing" of the decryption circuit in order to simplify decryption enough so that it is among the functions that the somewhat homomorphic scheme can homomorphically evaluate correctly. Squashing converts an SHE scheme into a bootstrappable SHE scheme. In [6], Brakerski and Vaikuntanathan use "dimension-modulus reduction" to simplify the decryption circuit and avoid squashing. Another way to remove squashing is given in [17].

In [4], Brakerski, Gentry, and Vaikuntanathan use "modulus switching" to reduce noise and lessen the need for bootstrapping. Modulus switching replaces a ciphertext mod p_1 with a ciphertext modulo a smaller modulus p_2 that decrypts to the same plaintext.

See [14] for a nice analogy ("Alice's jewelry store", with jewelry fabricated in nested secure gloveboxes) that gives the idea of FHE and bootstrapping. See also [22] for a good explanation of FHE for a general audience. See Vaikuntanathan's survey article [38] for a good description of modulus switching and other concepts from FHE.

3.1.6. *Malleability.* We remark that FHE schemes are always "malleable". In cryptography, malleability means that a ciphertext can be perturbed to create a new ciphertext that decrypts to a perturbation (in a known way) of the original plaintext. In a non-malleable encryption scheme, perturbing a ciphertext a little will generally produce an invalid ciphertext, i.e., one that does not decrypt to a valid plaintext. Malleability is often an undesirable property in cryptography. For example, if an auction uses encrypted bids, and (an adversary) Mallory sees the encryption of Bob's bid, one wants it to be the case that Mallory cannot construct a new ciphertext that decrypts to a bid that is one more than Bob's bid, i.e., one wants non-malleable encrypted bids.

There has been some work on obtaining partial or "targeted" non-malleability along with some limited homomorphic ability; see for example [33, 2]. There are interesting open questions in this area.

3.2. **Somewhat Homomorphic Encryption over the Integers.** We begin with a warm-up example from the introduction to [11]. This example of a somewhat homomorphic encryption scheme comes in two flavors, symmetric key and public key. To keep it short, we will be very imprecise about parameter choices and other details. For more information see [11].

We first give the symmetric key version. The shared key is an odd positive integer k. The message is a bit $m \in \{0, 1\}$. The encryptor chooses random integers q and r in a certain range, and so that $|2r| < k/2$, and computes the ciphertext

$$c = m + kq + 2r.$$

To decrypt, the decryptor computes ($c \bmod k$) $\bmod 2 = m$ where $a \bmod w$ means that one takes the representative of $a \bmod w$ in the range $(-w/2, w/2]$.

If $c_i = m_i + kq_i + 2r_i$ for $i = 1, 2$, then

$$c_1 + c_2 = (m_1 + m_2) + k(q_1 + q_2) + 2(r_1 + r_2),$$

$$c_1 \cdot c_2 = m_1 \cdot m_2 + k(m_1 q_2 + m_2 q_1 + k q_1 q_2 + 2 q_1 r_2 + 2 r_1 q_2) + 2(m_1 r_2 + r_1 m_2 + 4 r_1 r_2).$$

Thus the noise grows, and after one does too many multiplications or additions, the decryption function no longer outputs the correct plaintext. The ciphertexts also blow up in size. This Somewhat Homomorphic Encryption scheme is not fully homomorphic, but in [11] van Dijk et al. use Gentry's bootstrapping techniques to turn it into a Fully Homomorphic Encryption scheme.

A public key version, as in §3.1 of [11], is as follows. The secret key is again an odd positive integer k. The public key now consists of the integers $x_i = kq_i + 2r_i$ for $i = 0, 1, \ldots, t$, where the q_i and r_i are as before, so each x_i can be viewed as an encryption of 0 under the symmetric key scheme. The x_i are taken so that x_0 is the largest, x_0 is odd, and $x_0 \bmod k$ is even, where again $x \bmod k$ is in the interval $(-k/2, k/2]$.

To encrypt a message bit $m \in \{0, 1\}$, the encryptor chooses a random subset S of $\{1, \ldots, t\}$ and a random integer r in a certain range. The ciphertext is

$$c = m + 2 \sum_{i \in S} x_i + 2r \mod x_0.$$

The decryptor computes ($c \bmod k$) $\bmod 2 = m$.

The security is based on the difficulty of the Approximate Common Divisor Problem, which is the problem of finding k, given a collection of integers of the form $\{kq_i + r_i\}_{i=0}^{t}$ with r_i "small". Approximate Common Divisor Problems were introduced in [24] and have been studied in [7, 8].

3.3. **The Gentry, Smart-Vercauteren, and Gentry-Halevi SHE schemes.** We next give a version of the Somewhat Homomorphic Encryption schemes that were introduced by Gentry in [12, 13] and improved on by Smart and Vercauteren in [36] and by Gentry and Halevi in [16] (see also [28]). In these schemes, the public key corresponds to a "bad" (skewed) basis for a lattice, while the private key is a "good"

(more orthogonal) basis for the same lattice. The (N-dimensional) lattices are ideals in the ring of integers of the cyclotomic field of $2N$-th roots of unity. The plaintext is encoded as a (suitable) point in the ambient space $\mathbf{R}^N$. Encryption translates that point into the fundamental parallelepiped associated to the bad (public) basis. Decryption translates the ciphertext point into the fundamental parallelepiped associated to the good (private) basis. The security relies partly on the fact that it is difficult to find a good, nearly orthogonal basis for a given lattice.

We next give some of the details of a version of the scheme. Let

$$F(x) = x^N + 1 \in \mathbf{Z}[x]$$

with $N = 2^n$. Let θ be a root of $F(x)$; then θ is a primitive $2N$-th root of unity. Let

$$K = \mathbf{Q}[x]/\langle F(x)\rangle \cong \mathbf{Q}(\theta),$$

a CM-field of degree N over $\mathbf{Q}$. (A CM-field is a totally imaginary quadratic extension of a totally real number field. Examples include imaginary quadratic fields and cyclotomic fields. The K defined here is a cyclotomic field.) Let

$$v(x) = \sum_{i=0}^{N-1} v_i x^i \in \mathbf{Z}[x]$$

be a degree $N-1$ polynomial whose coefficients v_i are random t-bit integers for a suitably chosen t, and consider the $N \times N$ integral matrix

$$V = \begin{pmatrix} v_0 & v_1 & \cdots & v_{N-1} \\ -v_{N-1} & v_0 & \cdots & v_{N-2} \\ & & \cdots & \\ -v_1 & -v_2 & \cdots & v_0 \end{pmatrix}. \tag{1}$$

The rows of V are the coefficients of $x^i v(x) \bmod F(x)$ for $i = 0, \ldots, N-1$. Let L denote the lattice in $\mathbf{Z}^N$ generated by the rows of V, let $\gamma = v(\theta) \in K$, let $\mathrm{Norm}_{\mathrm{K}/\mathbf{Q}} : \mathrm{K} \to \mathbf{Q}$ denote the norm map, and let

$$d = \mathrm{Norm}_{\mathrm{K}/\mathbf{Q}}(\mathrm{v}(\theta)) = \mathrm{resultant}(\mathrm{F}, \mathrm{v}) = \det(\mathrm{V}) = \det(\mathrm{L}). \tag{2}$$

Replace the random polynomial $v(x)$ if necessary, until you have found one for which d is odd and square-free. (In [36], they start with $v(x) \equiv 1 \bmod 2\mathbf{Z}[x]$ to ensure that d is odd, and they replace $v(x)$, if necessary, until they find one for which d is prime. In [16] it is shown that it is not necessary for d to be prime; it suffices to have d odd and square-free.)

Whenever A is a matrix whose rows $\{\mathbf{a}_1, \ldots, \mathbf{a}_N\}$ form a $\mathbf{Z}$-basis for a lattice $L \subset \mathbf{R}^N$, define

$$P(A) = \Big\{ \sum_{i=1}^{N} \alpha_i \mathbf{a}_i : \alpha_i \in [-0.5, 0.5) \Big\},$$

a (half-open) parallelepiped. This is the "fundamental parallelepiped" associated to A. Every element of $\mathbf{R}^N/L$ has a unique representative in $P(A)$.

All reductions mod d will be taken in the range $[-d/2, d/2)$. Let $r \in [-d/2, d/2)$ denote the unique common root of $F(x)$ and $v(x)$ mod d. Let $r_i = r^i \pmod{d}$ and consider the $N \times N$ integral matrix

$$B = \begin{pmatrix} d & 0 & 0 & \cdots & 0 \\ -r_1 & 1 & 0 & \cdots & 0 \\ & \cdots & & & \\ -r_{N-1} & 0 & 0 & \cdots & 1 \end{pmatrix}. \tag{3}$$

Since d is odd and square-free, it follows that B is the Hermite Normal Form of the matrix V.

The public key now consists of d and r (or equivalently the matrix B), and the secret key is $v(x)$ (or the matrix V). To encrypt a bit $m \in \{0, 1\}$, choose a random noise polynomial $u(x) = \sum_{i=0}^{N-1} u_i x^i$ with each coefficient $u_i \in \{0, \pm 1\}$ taking values 1 and -1 with equal probability. Let $a(x) = m + 2u(x)$ and let

$$\mathbf{a} = (2u_0 + m, 2u_1, \ldots, 2u_{N-1})$$

be the vector of coefficients of $a(x)$. Let $\lceil \cdot \rfloor$ denote rounding to the nearest integer.

Let the ciphertext be

$$\mathbf{c} = \mathbf{a} - (\lceil \mathbf{a} B^{-1} \rfloor B) = (m + 2u(r) \mod d, 0, \ldots, 0),$$

which is the translation of $\mathbf{a}$ to the parallelepiped $P(B)$ (where translation means that one subtracts lattice vectors until one lands in the fundamental parallelepiped).

To decrypt a ciphertext $\mathbf{c}$, let

$$\mathbf{a}_1 = \mathbf{c} - (\lceil \mathbf{c} V^{-1} \rfloor V) = (a_0, \ldots, a_{N-1}),$$

which is the translation of $\mathbf{c}$ to the parallelepiped $P(V)$, and compute $m = a_0 \pmod 2$. As shown on p. 145 of [16], decryption works (i.e., $\mathbf{a}_1 = \mathbf{a}$) as long as the absolute value of every entry in $\mathbf{a} V^{-1}$ is less than $\frac{1}{2}$.

The rows of the matrix B are a "bad", i.e., skewed basis for the lattice L, while the rows of V are a "good" (secret) basis for L. If the rows of V are sufficiently orthogonal, and if the plaintext point $\mathbf{a}$ is chosen in a suitable way, then decryption yields the original plaintext point.

The scheme is homomorphic because its multiplication and addition are just multiplication and addition in the ring of integers of the field K.

The security of the above scheme is based on the simultaneous difficulty of the following problems.

The **Small Principal Ideal Problem (SPIP)** is the problem, given a principal ideal in either Hermite Normal Form (i.e., the matrix B) or two element representation (i.e., $\langle d, \theta - r \rangle$), of finding a "small" generator (e.g., $v(\theta)$) for it. If the SPIP is sufficiently hard, that would thwart a key recovery attack, wherein an adversary who knows the public key (B or (d, r)) tries to find the secret key ($v(x)$).

Security against an attack where the adversary tries to find the plaintext, given a ciphertext, is closely related to the difficulty of the **Closest Vector Problem** for

ideal lattices. This is the problem of finding a closest lattice point to a given point in the ambient space.

Another type of security is "semantic security". The requirement for semantic security is that an adversary, who is presented with a ciphertext that is either an encryption of 0 or an encryption of 1, cannot distinguish which it is with probability greater than $\frac{1}{2} + \varepsilon$ of getting the correct answer. The semantic security of the scheme is related to a new problem, that Smart and Vercauteren call the **Polynomial Coset Problem**. The Polynomial Coset Problem is the problem of distinguishing between a random element of $\mathbf{Z}/d\mathbf{Z}$ and an element of the form $f(r) \bmod d$, where $f(x) \in \mathbf{Z}[x]$ is random (and unknown) with small coefficients and r is the common root of $F(x)$ and $v(x) \bmod d$. The paper [36] states that the Polynomial Coset Problem is akin to Gentry's Ideal Coset Problem from [12]. These problems can be viewed as versions of the Bounded Distance Decoding problem from coding theory.

Gentry, Smart-Vercauteren and Gentry-Halevi "bootstrap" their somewhat homomorphic encryption schemes into fully homomorphic encryption schemes using a re-encryption algorithm. Making this cryptographically secure requires an additional security assumption, namely the difficulty of a decisional version of the **Sparse Subset-Sum Problem**, i.e., it should be difficult to distinguish between random subsets of $\mathbf{Z}/d\mathbf{Z}$ and those that have sparse subsets that sum to 0. Here, bootstrapping augments the public key with a "hint" about the secret key, namely, with a large set of vectors that has a very sparse subset that sums to the secret key.

4. Results and Discussion

We first give some observations concerning the Smart-Vercauteren (SV) and Gentry-Halevi (GV) schemes that were reviewed in Section 3.3 above. Our main result is a proposed variant of these schemes (see Section 4.6). We justify introducing this variant, and discuss some pros and cons in comparison to earlier schemes. This section represents joint work of Hendrik Lenstra and Alice Silverberg.

4.1. **Some comments on the SV and GH schemes.** We retain the notation of Section 3.3. The secret basis for the lattice L in the Smart-Vercauteren and Gentry-Halevi schemes consists of the rows of V, where the first row is chosen "at random". The more random, the higher the security, but the less likely that one can actually decrypt.

Our goal is to replace this secret basis with a nearly orthogonal set of vectors (and replace the lattice L with the lattice generated by these vectors). If the secret basis is nearly orthogonal, then decryption is feasible and amounts to finding a shortest vector in the coset $\mathbf{c} + L$, and security is maintained as long as there is still sufficient randomness.

With the Smart-Vercauteren and Gentry-Halevi schemes, decryption fails if the vector $\mathbf{a}$ does not lie in the parallelepiped $P(V)$. In this section we discuss some aspects of decryption, which motivated us to find a refinement of the SV and GH schemes in which decryption is more likely to succeed.

If $g(x) = \sum_{i=0}^{t} g_i x^i \in \mathbf{R}[x]$, let

$$||g(x)||_2 = \sqrt{\sum_{i=0}^{t} g_i^2} \quad \text{and} \quad ||g(x)||_\infty = \max_{i=0,\dots,t} |g_i|.$$

In [36, p. 427] it is shown that if the resultant d of (2) is roughly of size $||v(x)||_2^N \cdot ||F(x)||_2^m$, where $\deg(v) = m = N - 1$, then a quantity they call the decryption radius is sufficiently large to allow decryption. In Lemma 1 below we prove that the resultant d is at most $||v(x)||_2^N$, and therefore is not of size about $||v(x)||_2^N \cdot ||F(x)||_2^m$. In Lemma 2 we refine the bound in Lemma 1 of [36], in order to enable the decryption radius to be potentially sufficiently large to allow decryption.

(Note that the notation v, r, θ, d, and $a(x)$, which came from [16], is denoted G, α, ζ, p, and $C(x)$, respectively, in [36].)

Lemma 1. $d \le ||v(x)||_2^N$.

Proof. With θ a primitive $2N$-th root of unity as above, and taking the products and sum over all the roots ζ of $F(x)$, we have

$$d = \mathrm{Norm}_{\mathrm{K}/\mathbf{Q}}(\mathrm{v}(\theta)) = \prod_{\mathrm{F}(\zeta)=0} \mathrm{v}(\zeta) = \prod_{\mathrm{F}(\zeta)=0} (\mathrm{v}(\zeta)\mathrm{v}(\bar{\zeta}))^{1/2}$$

$$= \prod_{F(\zeta)=0} ((v(\zeta)\overline{v(\zeta)})^{1/N})^{N/2} \le \sum_{F(\zeta)=0} \left(\frac{v(\zeta)v(\bar{\zeta})}{N}\right)^{N/2} \quad (4)$$

where the inequality follows from the arithmetic-geometric mean inequality.

Since

$$\sum_{F(\zeta)=0} \zeta^k = \mathrm{Tr}_{K/\mathbf{Q}}(\theta^k) = \begin{cases} N & \text{if } k = 0, \\ 0 & \text{if } 0 < |k| < N, \end{cases}$$

we have

$$\sum_{F(\zeta)=0} v(\zeta)v(\overline{\zeta}) = (\sum_{i=0}^{N-1} v_i\theta^i)(\sum_i v_i\overline{\theta}^i) = \sum_{0\le i,j<N} v_iv_j\theta^{i-j} = N\sum_{i=0}^{N-1} v_i^2 = N||v(x)||_2^2.$$

The desired result follows by combining this with (4). □

The next result is a refinement of Lemma 1 of [36]. We recall that Lemma 1 of [36] stated that there exists a $Z(x) \in \mathbf{Z}[x]$ such that $Z(x)v(x) \equiv d \bmod F(x)$ and $||Z(x)||_\infty \le ||v(x)||_2^{N-1}||F(x)||_2^{N-1}$. (The $Z(x)$ obtained in Lemma 2 below is the same as the $Z(x)$ in Lemma 1 of [36].)

Lemma 2. *There exists a polynomial $Z(x) \in \mathbf{Z}[x]$ such that $Z(x)v(x) \equiv d \bmod F(x)$ and $||Z(x)||_\infty \le ||v(x)||_2^{N-1}$.*

Proof. As in [36], we apply Cramer's Rule and Hadamard's inequality. However, instead of applying the Hadamard inequality directly, we first do elementary operations to the Sylvester matrix that do not change its determinant d, and then apply Hadamard's inequality.

As in [36], there are polynomials

$$S(x) = \sum_{i=0}^{N-1} s_ix^i, \quad T(x) = \sum_{i=0}^{m-1} t_ix^i \quad \in \mathbf{Q}[x]$$

such that

$$S(x)v(x) + T(x)F(x) = 1.$$

Let $Z(x) = dS(x) = \sum_{i=0}^{N-1} z_ix^i \in \mathbf{Z}[x]$. Then

$$Z(x)v(x) \equiv d \bmod F(x).$$

As in [36] we have the matrix equation

$$\begin{pmatrix} v_m & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ v_{m-1} & v_m & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \ddots & \vdots \\ v_1 & v_2 & \cdots & 0 & 0 & 0 & \cdots & 1 \\ v_0 & v_1 & \cdots & v_m & 0 & 0 & \cdots & 0 \\ 0 & v_0 & \cdots & v_{m-1} & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & v_{m-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & v_0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} s_{N-1} \\ \vdots \\ \vdots \\ s_0 \\ t_{m-1} \\ \vdots \\ \vdots \\ t_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

where the first matrix is the Sylvester matrix $\mathrm{Syl}(v,F)^T$, an $(m+N)\times(m+N)$ matrix whose determinant is the resultant of v and F, which is d.

Suppose $1 \le j \le N$. As the first step in using Cramer's Rule to compute the j-th entry s_{N-j} of the vector of unknowns $(s_{N-1},\ldots,t_0)$, substitute the right hand vector of constants $(0,\ldots,0,1)^T$ for the j-th column of the matrix $\mathrm{Syl}(v,F)^T$.

Then for $i = 1,\ldots,N-1$, replace the i-th row of that matrix with that row minus the $(N+i)$-th row, so that the upper right $(N-1)\times(N-1)$ corner is a zero matrix. Then the determinant of the resulting matrix is the determinant of its upper left $(N-1)\times(N-1)$ submatrix, which by Cramer's Rule is $s_{N-j}\det(\mathrm{Syl}(v,F)) = ds_{N-j} = z_{N-j}$. Applying Hadamard's inequality to the columns, and using that the entries of the columns are the coefficients of $v(x)$, up to sign and permutation, we have that this determinant has absolute value at most $||v(x)||_2^{N-1}$, giving the desired result. □

We now examine the effect on decryption.

As on p. 426 of [36], define

$$\delta_\infty = \sup\{\frac{||g(x)h(x) \bmod F(x)||_\infty}{||g(x)||_\infty||h(x)||_\infty} : \deg(g),\deg(h) \le N\}.$$

Lemma 2 of [36] shows that for $F(x) = x^N + 1$ one has $\delta_\infty \le N$.

Define the decryption radius

$$\mathrm{r_{Dec}} = \frac{d}{2\delta_\infty||Z(x)||_\infty}$$

(following Lemma 1 of [28]). As in Lemma 1 of [28] and p. 425 of [36], decryption can be done if $||a(x)||_\infty < \mathrm{r_{Dec}}$. Using the refined bound $||Z(x)||_\infty \le ||v(x)||_2^{N-1}$ of Lemma 2 above and using that $\delta_\infty \le N$, we obtain

$$\mathrm{r_{Dec}} \ge \frac{d}{2N||v(x)||_2^{N-1}}. \tag{5}$$

If one knew that d were approximately $||v(x)||_2^N$, rather than just being bounded above by it as in Lemma 1, then using (5) would give

$$\mathrm{r_{Dec}} \ge \frac{d}{2N||v(x)||_2^{N-1}} \approx \frac{||v(x)||_2}{2N} \approx \frac{2^{\sqrt{N}-1}}{\sqrt{N}}.$$

However, if the resultant d is unexpectedly small and the coefficients of $Z(x)$ are sufficiently large, then $\mathrm{r_{Dec}}$ will be so small that decryption will not be possible. This is potentially a problem for the encryption scheme, motivating us to restrict the choice of the polynomial $v(x)$ in order to improve the ability to decrypt.

4.2. **Comments on a Gentry and Vercauteren variant of the SV and GH schemes.** To address the problem pointed out in the previous section, rather than taking $v_0,\ldots,v_{N-1}$ to be random t-bit integers as in [36, 16], Vercauteren (in email discussion with Lenstra) and Gentry (in conversation and email with Silverberg)

suggested taking v_0 to be approximately 2^t and taking the remaining v_i's of negligible size compared to 2^t, so that

$$(v_0, \ldots, v_{N-1}) \approx (2^t, 0, \ldots, 0).$$

The resulting basis is "mildly orthogonal" (in Gentry's words). In particular, it is orthogonal enough to allow decryption.

We next look briefly at the security of this variant. Let

$$R = \mathbf{Z}[\theta] \cong \mathbf{Z}[x]/(F(x)),$$

the ring of integers of the field K. Let

$$K_{\mathbf{R}} = K \otimes_{\mathbf{Q}} \mathbf{R} = R \otimes_{\mathbf{Z}} \mathbf{R} \cong \mathbf{C}^{N/2} \cong \mathbf{R}^N,$$

a Euclidean space, i.e., a finite dimensional vector space over $\mathbf{R}$ with a positive definite symmetric bilinear form.

Let $v = v(\theta) \approx v_0$. Then $L = Rv \cong \mathbf{Z}^N$ is a lattice in $K_{\mathbf{R}}$, and

$$d = \det(L) = \#(R/Rv) = \mathrm{Norm}_{\mathrm{K}/\mathbf{Q}}(\mathrm{v}) \approx |\mathrm{v_0}|^{\mathrm{N}}.$$

Thus, $d^{1/N}$ is approximately $|v_0|$. Let

$$\alpha = 1 \otimes d^{1/N} \in K_{\mathbf{R}}.$$

Then $||\alpha - v||$ is small. Recovering v amounts to solving the inhomogeneous approximation problem, with input α, to find the closest lattice vector v to α. However, if $v_1, \ldots, v_{N-1}$ are too small, then the closest lattice vector to α is *much* closer than the next closest lattice vector, so the LLL algorithm finds it.

4.3. **Gauss's general measure.** The scheme in [36] is analyzed there using the ℓ_2-norm $||g(x)||_2$. We instead use a norm that has some additional nice mathematical properties. When $F(x) = x^{2^n} + 1$ the two norms happen to coincide.

For now, take K to be any number field, let $N = [K : \mathbf{Q}]$, and let $K_{\mathbf{R}}$ denote the $\mathbf{R}$-algebra $K \otimes_{\mathbf{Q}} \mathbf{R}$. Define

$$q : K_{\mathbf{R}} \to \mathbf{R}^{\geq 0} \quad \text{by} \quad q(\beta) = \frac{1}{N} \sum_{\sigma : K_{\mathbf{R}} \hookrightarrow \mathbf{C}} \sigma(\beta)\overline{\sigma(\beta)} = \frac{1}{N} \sum_{\sigma : K_{\mathbf{R}} \hookrightarrow \mathbf{C}} |\sigma(\beta)|^2$$

where the bar denotes complex conjugation and the sum runs over all $\mathbf{R}$-algebra homomorphisms from $K_{\mathbf{R}}$ into $\mathbf{C}$.

The map q is a positive definite quadratic form on the $\mathbf{R}$-vector space $K_{\mathbf{R}}$, and q is canonical, independent of a choice of basis. The map q is (a renormalization of) the "general measure" of Gauss, and is sometimes called the T_2-norm. See [26] for some of its properties, especially in the case where K is a cyclotomic field.

The inner product on $K_{\mathbf{R}}$ associated to the quadratic form q is

$$\langle \beta, \beta' \rangle = \frac{q(\beta + \beta') - q(\beta) - q(\beta'))}{2}.$$

The length of β is

$$\sqrt{q(\beta)} = \sqrt{\langle \beta, \beta \rangle}. \tag{6}$$

The map q satisfies a Cauchy-Schwarz inequality:

$$|\langle \beta, \beta' \rangle| \leq \sqrt{q(\beta)}\sqrt{q(\beta')}. \tag{7}$$

When K is a CM or totally real number field, then for all $\beta \in K$ we have

$$q(\beta) = \frac{1}{N}\mathrm{Tr}_{K/\mathbf{Q}}(\beta\bar{\beta}) \in \mathbf{Q}.$$

From now on, suppose that $N = 2^n$, $F(x) = x^N + 1$, θ is a root of $F(x)$, and $K = \mathbf{Q}[x]/(F(x)) = \mathbf{Q}(\theta)$. Then $\overline{\sigma(\beta)} = \sigma(\overline{\beta})$ for all $\beta \in K$ (since K is a CM-field), and it follows that for all $\beta, \beta' \in K$ we have

$$\langle \beta, \beta' \rangle = \frac{1}{N}\mathrm{Tr}_{K/\mathbf{Q}}(\beta\overline{\beta'}) = \frac{1}{N}\sum_{\sigma : K \hookrightarrow \mathbf{C}} \sigma(\beta\overline{\beta'}). \tag{8}$$

This inner product is $\mathrm{Gal}(K/\mathbf{Q})$-equivariant. Further, if $\beta = \sum_{i=0}^{N-1} r_i\theta^i \in K_{\mathbf{R}}$ and $\beta(x) = \sum_{i=0}^{N-1} r_i x^i \in \mathbf{R}[x]/(F(x))$, then $q(\beta) = ||\beta(x)||_2^2$, as shown in the following lemma. This is one reason that the choice $F(x) = x^{2^n} + 1$ is a good one (note that q and $||\cdot||_2^2$ are not the same in general).

Lemma 3. *With $K = \mathbf{Q}(\theta)$ as above, let $S_\infty = \{$infinite primes of $K\}$, so that*

$$\mathbf{R}[x]/(F(x)) \cong K_{\mathbf{R}} \cong \mathbf{C}^{S_\infty}.$$

Identify $\beta \in K_{\mathbf{R}}$ with $\beta(x) = \sum_{i=0}^{N-1} r_i x^i \in \mathbf{R}[x]/(F(x))$ and with $(\beta_i)_{i \in S_\infty} \in \mathbf{C}^{S_\infty}$. Then

$$q(\beta) = \frac{1}{N}\sum_{\sigma : K_{\mathbf{R}} \hookrightarrow \mathbf{C}} |\sigma(\beta)|^2 = \frac{2}{N}\sum_{i \in S_\infty} \beta_i\overline{\beta_i} = \sum_{i=0}^{N-1} r_i^2 = ||\beta(x)||_2^2.$$

Proof. The second equality holds since each $i \in S_\infty$ corresponds to two embeddings σ. The third equality follows from the fact that the orthonormal basis $\{1, \theta, \ldots, \theta^{N-1}\}$ for $K_{\mathbf{R}}$ with respect to the inner product corresponding to q is identified with the basis $\{1, x, \ldots, x^{N-1}\}$ for $\mathbf{R}[x]/(F(x))$, which is an orthonormal basis with respect to the inner product $\langle \sum_{i=0}^{N-1} r_i x^i, \sum_{i=0}^{N-1} s_i x^i \rangle = \sum_{i=0}^{N-1} r_i s_i$, and so these inner products must coincide. □

4.4. **A first step.** In this section we give a first approximation to our variant of the SV and GH schemes, which we will revise in Section 4.6. Let

$$\lambda = \theta + \theta^{-1}$$

and let

$$K^+ = \mathbf{Q}(\lambda) \subset K = \mathbf{Q}(\theta) \cong \mathbf{Q}[x]/(x^{2^n} + 1).$$

Then K^+ is the totally real subfield of the CM-field K. Let

$$R^+ = \mathbf{Z}[\lambda],$$

the ring of integers of K^+. Then $R = \mathbf{Z}[\theta] = R^+ + \theta R^+$ since $\theta\lambda = \theta^2 + 1$.

Choose ρ_0 and ρ_1 in $R^+ = \mathbf{Z}[\lambda]$, "at random" in some suitable sense. Let

$$\rho = \rho_0 + \theta\rho_1 \in R, \qquad \gamma' = \rho/\bar{\rho} \in K. \tag{9}$$

Then

$$\gamma'\overline{\gamma'} = \frac{\rho}{\bar{\rho}} \cdot \frac{\bar{\rho}}{\rho} = 1.$$

Using the inner product given in (8), and the fact that $\gamma'\overline{\gamma'} = 1$, it is easy to see that

$$\langle \gamma'\theta^i, \gamma'\theta^j \rangle = \frac{1}{N}\mathrm{Tr}_{K/\mathbf{Q}}(\theta^{i-j}) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Thus, the set $\{\gamma'\theta^i\}_{i=0}^{N-1}$ is a set of vectors in K that is orthonormal with respect to the inner product $\langle\ ,\ \rangle$.

However, γ' is not necessarily in R, and the cryptosystems require elements of R. So let

$$\gamma = M\gamma' + 1 \in R$$

where $M \in \mathbf{Z}$ is chosen so that $M\gamma' \in R$ (for example, one could take $M = \rho\bar{\rho}$), so that $d = \mathrm{Norm}_{\mathrm{K}/\mathbf{Q}}(\gamma)$ is odd, and so that $R/\gamma R \cong \mathbf{Z}/d\mathbf{Z}$. Let

$$L = \gamma R,$$

the ideal lattice in R generated by γ.

As in Section 3.3, the private key is γ and the public key consists of d and r. Since $\{\gamma\theta^i\}_{i=0}^{N-1}$ is a nearly orthogonal basis for the lattice L, decryption is likely to be feasible.

4.5. **Discussion of security of the first step.** To what extent does this additional mathematical structure weaken the security of the scheme?

Before, the secret key $v(x)$ had N degrees of freedom, corresponding to the N coefficients of $v(x)$. Now there are $N/2$ degrees of freedom. This can be seen as follows. Choose ρ_1 suitably random in the degree $N/2$ number field $\mathbf{Q}(\lambda)$ and let $\rho = 1 + \theta\rho_1$. Multiplying by an element of $\mathbf{Q}(\lambda)^\times$ to get something of the form $\rho_0 + \theta\rho_1$ does not change $\gamma' = \rho/\bar{\rho}$.

Further, $\gamma\overline{\gamma}$ is a totally positive element of R^+, and

$$d = \mathrm{Norm}_{\mathrm{K}/\mathbf{Q}}(\gamma) = \prod_{\sigma:\mathrm{K}^+\hookrightarrow\mathbf{R}} \sigma(\gamma\overline{\gamma}) \in \mathbf{R}^{>0}$$

where σ runs through the $N/2$ embeddings of the field K^+ in $\mathbf{R}$.

Letting

$$\delta = \gamma - 1 = M\gamma' \in R,$$

then

$$\delta\overline{\delta} = (\gamma - 1)(\overline{\gamma} - 1) = M^2 \in R^+$$

(since $\gamma'\overline{\gamma'} = 1$) and

$$\mathrm{Norm}_{\mathrm{K}/\mathbf{Q}}(\delta) = \mathrm{M}^{\mathrm{N}},$$

an N-th power that is close to the public information $d = \mathrm{Norm}_{\mathrm{K}/\mathbf{Q}}(\gamma)$. Thus d is approximately M^N, so M is approximately $\sqrt[N]{d}$. Rounding $\sqrt[N]{d}$ to the nearest integer might yield M, and therefore also $\delta\overline{\delta}$. So the public information leaks information about $\delta\overline{\delta}$. Is this dangerous? That's not clear, so next we will try to do better.

4.6. **A proposal for a somewhat homomorphic encryption scheme.** To play it safer, we will take $\gamma = M\gamma' + e$, where $e \in R \cong \mathbf{Z}[x]/(F(x))$ is chosen so that the polynomial has small coefficients picked at random from too large a set to be guessable. The idea will be to take e small enough so that $\{\gamma\theta^i\}_{i=0}^{N-1}$ is still an almost orthogonal basis for the lattice L (i.e., so that $M\gamma'$ is still the dominant term). The randomness in the choice of e adds to the security, in comparison to just taking $e = 1$. The variant of the SV and GH schemes mentioned in Section 4.2 can be viewed as a special case of the proposed scheme, but now we choose $v(x)$ from a larger set, giving potentially greater security. In Section 4.7 we will justify our choice of the set from which e is taken, and will justify our lower bound on the size of the integer M. We next give the details.

With γ' as in (9), take $M \in \mathbf{Z}$ so that $M\gamma' \in R$ and $M > 4N$. Choose $e \in R$ at random subject to the restriction that $\sqrt{q(e)} < (\sqrt{1 + \frac{1}{2N}} - 1)M$. Let

$$\gamma = M\gamma' + e$$

and let $d = \mathrm{Norm}_{\mathrm{K}/\mathbf{Q}}(\gamma)$.

Write $\gamma = \sum_{i=0}^{N-1} v_i\theta^i$ with $v_i \in \mathbf{Z}$, let $v(x) = \sum_{i=0}^{N-1} v_i x^i \in \mathbf{Z}[x]$, and let V be the matrix associated to $v(x)$ as in (1) above. Check that d is odd and that $R/\gamma R \cong \mathbf{Z}/d\mathbf{Z}$. To check the latter, as in §3 of [16], compute $w(x) = \sum_{i=0}^{N-1} w_i x^i \in \mathbf{Z}[x]$ such that $w(x)v(x) = d \pmod{F(x)}$ and let $r = w_0/w_1 \pmod{d}$ (if $\gcd(w_1, d) = 1$), where as usual $r \in \mathbf{Z}$ is taken in the interval $[-d/2, d/2)$. Check that $r^N \equiv -1 \pmod{d}$. If so, then (as in §3 of [16]) the Hermite Normal Form B of the matrix V is of the form in equation (3). If any step above fails, start again with a new e (and possibly M).

The private key is $\gamma \in R$.

The public key consists of d and r.

To encrypt a message bit $b \in \{0, 1\}$, choose random integers $a_0, \ldots, a_{N-1}$ in the range $[\frac{-M}{2\sqrt{N+1}}, \frac{M}{2\sqrt{N+1}}]$ and adjust them so that

$$\#\{i : a_i \text{ is odd}\} \equiv b \pmod{2}.$$

Let $\mathbf{a} = (a_0, \ldots, a_{N-1}) \in \mathbf{Z}^N$.

As before, let the ciphertext $\mathbf{c}$ be the translation of $\mathbf{a}$ to the parallelepiped $P(B)$, i.e.,

$$\mathbf{c} = \mathbf{a} - (\lceil \mathbf{a}B^{-1} \rfloor B).$$

As before, to decrypt a ciphertext $\mathbf{c}$, let $\mathbf{a}_1$ be the translation of the ciphertext $\mathbf{c}$ to the parallelepiped $P(V)$, i.e.,

$$\mathbf{a}_1 = \mathbf{c} - (\lceil \mathbf{c}V^{-1} \rfloor V) = (a'_0, \ldots, a'_{N-1}).$$

Let

$$b = \#\{i : a'_i \text{ is odd}\} \pmod 2.$$

By Corollary 10 below we have $\mathbf{a} \in P(V)$, so $\mathbf{a} = \mathbf{a}_1$ and decryption is successful.

4.7. **Justification of parameter choices.** In this section we justify the conclusion that $\mathbf{a} \in P(V)$, and we justify our choices $M \geq 4N + 1$, $\sqrt{q(e)} < (\sqrt{1 + \frac{1}{2N}} - 1)M$, and $|a_i| \leq \frac{M}{2\sqrt{N+1}}$.

Definition 4. If $A = (a_{ij})$ is an $N \times N$ matrix with real entries, define

$$||A|| = \max_{i,j} |a_{ij}|.$$

Matrix multiplication shows that whenever E and F are $N \times N$ matrices with real entries, then

$$||EF|| \leq N||E|| \cdot ||F||. \tag{10}$$

Write I_N for the $N \times N$ identity matrix.

Lemma 5. *Suppose A is an $N \times N$ matrix with real entries, $\delta \in \mathbf{R}$, $0 \leq \delta < 1$, and*

$$||A - I_N|| \leq \frac{\delta}{N}.$$

Then A is invertible, and

$$||A^{-1} - I_N|| \leq \frac{\delta}{N(1-\delta)}.$$

Proof. Let $D = I_N - A$. Then $||D|| \leq \frac{\delta}{N}$. By (10) we have $||D^i|| \leq \frac{\delta^i}{N}$. Since $\frac{\delta^i}{N} \to 0$ as $i \to \infty$, we have

$$A^{-1} = I_N + D + D^2 + D^3 + \ldots$$

and

$$||A^{-1} - I_N|| \leq \sum_{i \geq 1} \frac{\delta^i}{N} = \frac{\delta}{N(1-\delta)}.$$

□

Proposition 6. *Suppose (L, q) is a lattice of rank N, and $\langle\ ,\ \rangle$ is the inner product associated to q, and $\{b_1, \ldots b_N\}$ is a $\mathbf{Z}$-basis for L. Let $C = (\langle b_i, b_j \rangle)_{i,j}$ denote the associated $(N \times N)$ Gram matrix. Suppose that $m \in \mathbf{R}^+$, that $\epsilon \in \mathbf{R}^{\geq 0}$, that*

$$||C - mI_N|| \leq \epsilon,$$

and that $\epsilon < m/N$. Suppose $\alpha \in L \otimes_{\mathbf{Z}} \mathbf{R} = \mathbf{R}L$ and write $\alpha = \sum_{i=1}^{N} \alpha_i b_i$ with $\alpha_i \in \mathbf{R}$. Then for $i = 1, \ldots, N$ we have

$$|\alpha_i|^2 \leq \frac{q(\alpha)}{m}\big(1 + \frac{\epsilon}{m - N\epsilon}\big).$$

Proof. Let $\{b_i^\dagger\}_{i=1}^N$ denote the dual basis of $L \otimes_{\mathbf{Z}} \mathbf{R}$ to the basis $\{b_i\}_{i=1}^N$, i.e., $\langle b_i^\dagger, b_j \rangle = \delta_{ij}$ where δ_{ij} is Kronecker's delta. Let $C^\dagger = (\langle b_i^\dagger, b_j^\dagger \rangle)_{i,j}$, an $N \times N$ matrix with real entries. It is an exercise to show that $C^\dagger = C^{-1}$.

Since $||C - mI_N|| \leq \epsilon$, it follows that $||m^{-1}C - I_N|| \leq \epsilon/m$. Applying Lemma 5 with $A = m^{-1}C$ and $\delta = N\epsilon/m$ gives

$$||mC^\dagger - I_N|| \leq \frac{\epsilon}{m - N\epsilon}.$$

Thus

$$||C^\dagger - \frac{1}{m} I_N|| \leq \frac{\epsilon}{m(m - N\epsilon)}$$

yielding

$$||C^\dagger|| \leq \frac{1}{m}\big(1 + \frac{\epsilon}{m - N\epsilon}\big). \tag{11}$$

Further, $\langle b_i^\dagger, \alpha \rangle = \sum_{j=1}^{N} \alpha_j \langle b_i^\dagger, b_j \rangle = \alpha_i$. Now by the Cauchy-Schwarz inequality (7) and by (6),

$$|\alpha_i| = |\langle b_i^\dagger, \alpha \rangle| \leq \sqrt{q(b_i^\dagger)}\sqrt{q(\alpha)} = \sqrt{q(\alpha)}\sqrt{\langle b_i^\dagger, b_i^\dagger \rangle}.$$

Using (11) we now have

$$|\alpha_i|^2 \leq q(\alpha)\langle b_i^\dagger, b_i^\dagger \rangle \leq q(\alpha)||C^\dagger|| \leq \frac{q(\alpha)}{m}\big(1 + \frac{\epsilon}{m - N\epsilon}\big)$$

as desired. □

Lemma 7. *As usual, let θ be a root of $x^{2^n} + 1$, let $K = \mathbf{Q}(\theta)$, and let $R = \mathbf{Z}[\theta]$. Suppose that $M \in \mathbf{Z}^{>0}$, $\gamma' \in K$, and $e \in R$, and suppose that $\gamma'\overline{\gamma'} = 1$ and $M\gamma' \in R$. Let $\gamma = M\gamma' + e \in R$. Define q and $\langle\ ,\ \rangle$ as in Section 4.3 and let δ_{ij} denote Kronecker's delta. For $i = 1, \ldots, N$, let $b_i = \gamma\theta^{i-1}$. Then for all i and j in $\{1, \ldots, N\}$ we have*

$$|\langle b_i, b_j \rangle - M^2\delta_{ij}| \leq 2M\sqrt{q(e)} + q(e).$$

Proof. Note that $\langle \theta^i, \theta^j \rangle = \delta_{ij}$ and $\langle \gamma'\theta^i, \gamma'\theta^j \rangle = \delta_{ij}$ as before, so $q(\theta^i) = \langle \theta^i, \theta^i \rangle = 1$ and $q(\gamma'\theta^i) = \langle \gamma'\theta^i, \gamma'\theta^i \rangle = 1$. We then have

$$\begin{aligned}
|\langle b_i, b_j \rangle - M^2\delta_{ij}| &= |\langle M\gamma'\theta^{i-1} + e\theta^{i-1}, M\gamma'\theta^{j-1} + e\theta^{j-1} \rangle - M^2\delta_{ij}| \\
&= |\langle M\gamma'\theta^{i-1}, e\theta^{j-1} \rangle + \langle e\theta^{i-1}, M\gamma'\theta^{j-1} \rangle + \langle e\theta^{i-1}, e\theta^{j-1} \rangle| \\
&\leq M|\langle \gamma'\theta^{i-1}, e\theta^{j-1} \rangle| + M|\langle e\theta^{i-1}, \gamma'\theta^{j-1} \rangle| + |\langle e\theta^{i-1}, e\theta^{j-1} \rangle| \\
&\leq 2M\sqrt{q(e)} + q(e)
\end{aligned}$$

where the last inequality follows from the Cauchy-Schwarz inequality (7) and the equalities $q(\gamma'\theta^i) = 1$ and $q(\theta^i) = 1$. □

Theorem 8. *Suppose θ, M, γ', e, γ, and q are as in Lemma 7. Suppose $\alpha = \sum_{i=0}^{N-1} \alpha_i \gamma\theta^i$ with $\alpha_i \in \mathbf{R}$. Suppose $0 < c < 1$ and*

$$\sqrt{q(e)} < (\sqrt{1 + \frac{c}{N}} - 1)M. \tag{12}$$

Then

$$|\alpha_i|^2 < \frac{q(\alpha)}{M^2}(1 + \frac{2M\sqrt{q(e)} + q(e)}{M^2(1-c)}).$$

Proof. Let $\epsilon = 2M\sqrt{q(e)} + q(e)$. Then (12) holds if and only if $\epsilon < cM^2/N$, as follows:

$$\epsilon - cM^2/N = 2M\sqrt{q(e)} + q(e) - cM^2/N = (\sqrt{q(e)} + M)^2 - (1 + c/N)M^2.$$

So $\epsilon < cM^2/N$ if and only if $(\sqrt{q(e)} + M)^2 < (1 + c/N)M^2$. Now take square roots.

By Lemma 7 we can apply Proposition 6 with $m = M^2$, giving

$$|\alpha_i|^2 \leq \frac{q(\alpha)}{M^2}(1 + \frac{\epsilon}{M^2 - N\epsilon}) < \frac{q(\alpha)}{M^2}(1 + \frac{\epsilon}{M^2(1-c)})$$

as desired, where the last inequality uses that $\epsilon < cM^2/N$. □

Remark 9. With hypotheses as in Theorem 8, if one takes α so that

$$q(\alpha) \leq \frac{M^2}{4[1 + \frac{c}{N(1-c)}]}$$

and uses that $2M\sqrt{q(e)} + q(e) = \epsilon < cM^2/N$, then Theorem 8 gives that $|\alpha_i| < 1/2$ for all i.

Corollary 10. *Suppose θ, M, γ', e, γ, and q are as in Lemma 7, and suppose that*

$$\sqrt{q(e)} < (\sqrt{1 + \frac{1}{2N}} - 1)M.$$

Suppose $\alpha = \sum_{i=0}^{N-1} a_i\theta^i = \sum_{i=0}^{N-1} \alpha_i\gamma\theta^i$ with $a_i, \alpha_i \in \mathbf{R}$. Let $A = \max_i |a_i| \in \mathbf{R}^{\geq 0}$ and suppose

$$A \leq \frac{M}{2\sqrt{N+1}}. \tag{13}$$

Then $|\alpha_i| < 1/2$.

Proof. Take $c = 1/2$ in Theorem 8, and use Theorem 8 and that $2M\sqrt{q(e)} + q(e) = \epsilon < cM^2/N = M^2/(2N)$, to obtain

$$|\alpha_i|^2 < \frac{q(\alpha)}{M^2}(1 + \frac{2\epsilon}{M^2}) < \frac{q(\alpha)}{M^2}(1 + \frac{1}{N}).$$

By Lemma 3 and the definition of A we have $q(\alpha) \leq NA^2$. Now apply (13). □

Remark 11. Since $1 + \frac{1}{2N}$ is approximately $(1 + \frac{1}{4N})^2$, we have that

$$(\sqrt{1 + \frac{1}{2N}} - 1)M \approx \frac{M}{4N}.$$

So the upper bound on $\sqrt{q(e)}$ in the above results forces $M \gg N$. Taking $M > 2N + \sqrt{2N(2N+1)}$ (or more simply $M \geq 4N+1$) ensures that $(\sqrt{1 + \frac{1}{2N}} - 1)M > 1$.

4.8. **Discussion of security.** Recall that $\gamma = M\gamma' + e$ and $\gamma'\overline{\gamma'} = 1$. Let $L^+ = \mathrm{Norm}_{\mathrm{K/K^+}}(\mathrm{L})$, an ideal in R^+. Then L^+ is a lattice in the Euclidean space

$$E^+ = R^+ \otimes_{\mathbf{Z}} \mathbf{R} \cong \mathbf{R}^{N/2},$$

and

$$\gamma\overline{\gamma} \in (\gamma\overline{\gamma})R^+ = L^+ \cong \mathbf{Z}^{N/2}.$$

Since K is a CM-field, we have $\sigma(\gamma'\overline{\gamma'}) = 1$ for all $\sigma : K \hookrightarrow \mathbf{C}$, and

$$d = \mathrm{Norm}_{\mathrm{K/}\mathbf{Q}}(\gamma) = \prod_{\sigma:\mathrm{K}\hookrightarrow\mathbf{C}} \sigma(\gamma) = \prod_{\tau:\mathrm{K}^+\hookrightarrow\mathbf{R}} \tau(\gamma\overline{\gamma}).$$

For each real embedding $\tau : K^+ \hookrightarrow \mathbf{R}$, the size of $\tau(\gamma\overline{\gamma})$ is close to $d^{2/N}$. Let

$$\alpha^+ = 1 \otimes d^{2/N} \in E^+.$$

Then α^+ is close to $\gamma\overline{\gamma}$. With a sufficiently good inhomogeneous approximation algorithm one could recover $\gamma\overline{\gamma}$ from α^+. Analyzing known attacks comes down to the question of how good the LLL algorithm is at solving inhomogeneous approximation problems. If $q(\frac{e}{M})$ were too small, LLL would recover $\gamma\overline{\gamma}$, though it is not clear how much this would help to recover γ. Even if one learns $\gamma\overline{\gamma}$ and $\delta\overline{\delta}$ (with $\delta = \gamma - 1$ as in Section 4.5), if e is unknown one still does not know δ or γ.

Gentry points out in his PhD thesis [13, p. 68] that the NTRU signature attack in the Gentry-Szydlo paper [20] provides an attack on certain ideal lattices in certain rings of the form $\mathbf{Z}[x]/(x^N - 1)$ that have an orthonormal basis. More work is needed to determine whether such an attack can be used to weaken the security of the scheme presented here.

5. Conclusions

The mathematical foundations for certain Somewhat Homomorphic Encryption schemes are studied and developed, and strengths and weaknesses are discovered. In addition, Lenstra and Silverberg propose lattices with nearly orthogonal bases, for use in Fully Homomorphic Encryption. These bases, when used as the secret key in a Fully Homomorphic Encryption scheme, are designed to allow efficient decryption. Justification is given that this choice provides a better balance of security and efficiency than related previously proposed lattice-based Fully Homomorphic Encryption schemes. Further work is needed to quantify the security of Fully Homomorphic Encryption schemes that are based on lattices that have nearly orthogonal bases.

6. Recommendations

In order to give convincing evidence that methods for computing on encrypted data are cryptographically secure, it is important to discover, develop, and understand the mathematical foundations on which these methods rely. This will enable the construction of more efficient and secure systems, and will give reliable information and confidence as to which systems are secure. Recent proposals for secure computing on encrypted data make use of lattices that have some symmetry. Therefore, the primary recommendation is that the mathematical foundations of lattices with symmetry be discovered and developed. An additional recommendation is that the security of homomorphic encryption schemes based on ideal lattices be quantified, in order to give confidence in the security of such schemes and in order to be able to effectively compare different schemes.

Bibliography

[1] D. Boneh, E-J. Goh, and K. Nissim, *Evaluating 2-DNF formulas on ciphertexts*, in Theory of Cryptography—TCC'05, Lect. Notes in Comp. Sci. **3378** (2005), Springer, 325-341.

[2] D. Boneh, G. Segev, and B. Waters, *Targeted malleability: homomorphic encryption for restricted computations*, Innovations in Theoretical Computer Science 2012 (ITCS 2012), ACM (2012), 350–366.

[3] Z. Brakerski, *Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP*, in Advances in Cryptology—CRYPTO 2012, Lect. Notes in Comp. Sci. **7417** (2012), Springer, 868–886.

[4] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, *(Leveled) fully homomorphic encryption without bootstrapping*, in Innovations in Theoretical Computer Science (ITCS) 2012, ACM, 309–325.

[5] Z. Brakerski and V. Vaikuntanathan, *Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages*, in Advances in Cryptology—CRYPTO 2011, Lect. Notes in Comp. Sci. **6841** (2011), Springer, 505–524.

[6] Z. Brakerski and V. Vaikuntanathan, *Efficient Fully Homomorphic Encryption from (Standard) LWE*, in IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS) (2011), Rafail Ostrovsky (ed.), IEEE, 97–106.

[7] Y. Chen and P. Q. Nguyen, *Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers*, in Advances in Cryptology—EUROCRYPT 2012, Lect. Notes in Comp. Sci. **7237** (2012), Springer, 502–519.

[8] H. Cohn and N. Heninger, *Approximate common divisors via lattices*, to appear in Algorithmic Number Theory (ANTS X), Mathematical Sciences Publishers; `http://arxiv.org/abs/1108.2714`.

[9] J-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, *Fully homomorphic encryption over the integers with shorter public keys*, in Advances in Cryptology—CRYPTO 2011, Lect. Notes in Comp. Sci. **6841** (2011), Springer, 487-504.

[10] J-S. Coron, D. Naccache, and M. Tibouchi, *Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers*, in Advances in Cryptology—EUROCRYPT 2012, Lect. Notes in Comp. Sci. **7237** (2012), Springer, 446–464.

[11] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, *Fully Homomorphic Encryption over the Integers*, in Advances in Cryptology—EUROCRYPT 2010, Lect. Notes in Comp. Sci. **6110** (2010), Springer, 24–43.

[12] C. Gentry, *Fully homomorphic encryption using ideal lattices*, in Proceedings of the 41st ACM Symposium on Theory of Computing—STOC 2009, ACM, New York (2009), M. Mitzenmacher (ed.), 169–178.

[13] C. Gentry, *A fully homomorphic encryption scheme*, Stanford University PhD thesis, 2009, `http://crypto.stanford.edu/craig/craig-thesis.pdf`.

[14] C. Gentry, *Computing arbitrary functions of encrypted data*, Communications of the ACM **53** (2010), 97–105.

[15] C. Gentry, *Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness*, in Advances in Cryptology—CRYPTO 2010, Lect. Notes in Comp. Sci. **6223** (2010), Springer, 116–137.

[16] C. Gentry and S. Halevi, *Implementing Gentry's fully-homomorphic encryption scheme*, in Advances in Cryptology—EUROCRYPT 2011, Lect. Notes in Comp. Sci. **6632** (2011), K. G. Paterson (ed.), Springer, 129–148.

[17] C. Gentry and S. Halevi, *Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits*, in IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS) (2011), Rafail Ostrovsky (ed.), IEEE, 107–116.

[18] C. Gentry, S. Halevi, and N. P. Smart, *Better Bootstrapping in Fully Homomorphic Encryption*, Public Key Cryptography 2012, 1–16.

[19] C. Gentry, S. Halevi, and N. P. Smart, *Fully Homomorphic Encryption with Polylog Overhead*, in Advances in Cryptology—EUROCRYPT 2012, Lect. Notes in Comp. Sci. , (2012), Springer, 465–482.

[20] C. Gentry and M. Szydlo, *Cryptanalysis of the revised NTRU signature scheme*, Advances in Cryptology–EUROCRYPT 2002 Lect. Notes in Comp. Sci. **2332** (2002), Lars R. Knudsen (ed.), Springer, 299-320.

[21] S. Goldwasser and S. Micali, *Probabilistic encryption and how to play mental poker keeping secret all partial information*, Proceedings of the 14th ACM Symposium on Theory of Computing—STOC 1982, ACM (1982), 365-377.

[22] B. Hayes, *Alice and Bob in Cipherspace*, American Scientist **100** (2012), 362–367.

[23] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, in Proceedings of ANTS-III—Algorithmic Number Theory Third International Symposium, Joe P. Buhler (ed.), Lect. Notes in Comp. Sci. **1423**, (1998), Springer, 267–288.

[24] N. Howgrave-Graham, *Approximate integer common divisors*, in Cryptography and Lattices, International Conference, CaLC 2001, Lect. Notes in Comp. Sci. **2146** (2001), Springer, 51-66.

[25] K. Lauter, M. Naehrig, and V. Vaikuntanathan, *Can homomorphic encryption be practical?*, in Proceedings of the 3rd ACM Cloud Computing Security Workshop, CCSW 2011, ACM, New York, 113–124.

[26] H. W. Lenstra, Jr., *Euclid's algorithm in cyclotomic fields*, J. London Math. Soc. (2) **10** (1975), no. 4, 457-465.

[27] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515-534.

[28] J. Loftus, A. May, N. P. Smart, F. Vercauteren, *On CCA-Secure Somewhat Homomorphic Encryption*, in Selected Areas in Cryptography 2011, Lect. Notes in Comp. Sci. **7118** (2012), A. Miri and S. Vaudenay (eds.), Springer, 55–72.

[29] A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan, *On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption*, in Proceedings of the 44th ACM Symposium on Theory of Computing—STOC 2012, ACM, New York, 1219–1234.

[30] V. Lyubashevsky, C. Peikert, and O. Regev, *On Ideal Lattices and Learning with Errors over Rings*, in EUROCRYPT 2010, Lect. Notes in Comp. Sci. **6110** (2010), Springer, 1–23.

[31] P. Paillier, *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*, in Advances in Cryptology—EUROCRYPT '99, Lect. Notes in Comp. Sci. **1592** (1999), Springer, 223–238.

[32] C. Peikert, *Public-key cryptosystems from the worst-case shortest vector problem*, in Proceedings of the 41st ACM Symposium on Theory of Computing—STOC 2009, ACM, New York, 333-342.

[33] M. Prabhakaran and M. Rosulek, *Homomorphic Encryption with CCA Security*, in Automata, Languages and Programming, ICALP 2008, Lect. Notes in Comp. Sci. **5126** (2008), Luca Aceto et al. (eds.), Springer, 667–678.

[34] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, in Proceedings of the 37th ACM Symposium on Theory of Computing—STOC 2005, ACM, New York, 84-93; full version in Journal of the ACM **56** (2009), Article 34.

[35] R. Rivest, L. Adleman, and M. Dertouzos, *On Data Banks and Privacy Homomorphisms*, in Foundations of Secure Computation, R. DeMillo, D. Dobkin, A. Jones, and R. Lipton (eds.), Academic Press, New York (1978), 169–180.

[36] N. P. Smart and F. Vercauteren, *Fully homomorphic encryption with relatively small key and ciphertext sizes*, in Public Key Cryptography— PKC 2010, Lect. Notes in Comp. Sci. **6056**, (2010), P. Q. Nguyen and D. Pointcheval (eds.), Springer, 420–443.

[37] D. Stehlé and R. Steinfeld, *Faster fully homomorphic encryption*, in Advances in Cryptology—ASIACRYPT 2010, Lect. Notes in Comp. Sci. **6477** (2010), M. Abe (ed.), Springer, 377-394.

[38] V. Vaikuntanathan, *Computing Blindfolded: New Developments in Fully Homomorphic Encryption*, in IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS) (2011), Rafail Ostrovsky (ed.), IEEE, 5–16.

List of Symbols, Abbreviations, and Acronyms

$\mathbf{C}$	the complex numbers
FHE	Fully Homomorphic Encryption
$\mathbf{F}_q$	the finite field with q elements
GH	Gentry-Halevi Somewhat Homomorphic Encryption scheme
LLL	Lenstra-Lenstra-Lovász lattice basis reduction algorithm
$\mathbf{Q}$	the rational numbers
$\mathbf{R}$	the real numbers
SHE	Somewhat Homomorphic Encryption
SPIP	Small Principal Ideal Problem
SV	Smart-Vercauteren Somewhat Homomorphic Encryption scheme
$\mathbf{Z}$	the integers